IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS:	Oliver et al.
APPLICATION NO.:	10/776,677
FILING DATE:	February 10, 2004
TITLE:	Message Classification
EXAMINER:	Unknown
ART UNIT:	2141
ATTY.DKT.NO.:	PA3630US

CERTIFICATE OF MAILING UNDER 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, postage prepaid, in an envelope addressed to Mail Stop Petition, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on **July 26, 2006**.

Karen L. Kaufman

MAIL STOP PETITION
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

PETITION TO MAKE SPECIAL IN ACCORDANCE WITH

37 C.F.R. § 1.102(D) AND MPEP § 708.02(VIII)

SIR:

The Applicants respectfully request the Examiner advance the present application out of turn for examination (accelerated examination) through the submission of the present petition. This petition is presented in accordance with 37 C.F.R. § 1.102(d) and the conditions set forth for such a petition as detailed in MPEP § 708.02(VIII).

I. MPEP § 708.02(VIII)

MPEP § 708.02(VIII) notes that "[a] new application (one which has not received any examination by the examiner) may be granted special status." MPEP § 708.02(VIII). The Applicants declare that the present application is new in that it has not received any examination by the examiner and is thus eligible for special status. Granting of special status is respectfully requested.

II. MPEP § 708.02(VIII)(A)

MPEP § 708.02(VIII)(A) requires the applicant "[s]ubmit[ ] a petition to make special accompanied by the fee set forth in 37 CFR 1.17(h)." MPEP § 708.02(VIII)(A). The Applicants submit the present petition to make special by means of accelerated examination. The fee set forth by 37 C.F.R. § 1.17(h) is satisfied by the enclosed check. The Examiner has been authorized to charge any additional fee due to Deposit Account 06-0600 through the enclosed Form PTO-SB-17p, which is presented in duplicate.

III. MPEP § 708.02(VIII)(B)

MPEP § 708.02(VIII)(B) requires "all claims [be] directed to a single invention." MPEP § 708.02(VIII)(B). Alternatively, if all the claims in an application presented for a grant of special status are not directed toward a single invention as determined by the Office, the applicants are required to "make an election without traverse as a prerequisite to the grant of special status." MPEP § 708.02(VIII)(B). The Applicants believe that all claims presented in this application are directed to a single invention. If the Office makes a determination that the claims are not directed toward a single invention and to facilitate any election—if necessary—the Applicants hereby elect any claim set associated with claim 1 of the present application, such an election being without traverse.

IV. MPEP § 708.02(VIII)(C)

The Applicants hereby declare that a pre-examination search has been made as required by MPEP § 708.02(VIII)(C). The pre-examination search was directed toward the invention as claimed in the application and in the following fields:

A. United States Patent and Trademark Office Full-Text Database

The United States Patent and Trademark Office Full-Text database for both issued patents and pending publications was searched in the following classes and subclasses:

- Class 380, Subclass 1 for Cryptography; Cryptanalysis;
- Class 380, Subclass 2 for Cryptography; Equipment Test or Malfunction Indication;
- Class 700, Subclass 55 for Data Processing: General Control Systems or Specific Applications; Filtering;
- Class 707, Subclass 6 for Data Processing: Database and File Management or Data Structures; Pattern Matching Access;
- Class 707, Subclass 7 for Data Processing: Database and File Management or Data Structures; Sorting;
- Class 708, Subclass 306 for Electrical Computers: Arithmetic Processing and Calculating; Finite Arithmetic Effect;
- Class 708, Subclass 525 for Electrical Computers: Arithmetic Processing and Calculating; Status Condition/Flag Generation or Use;
- Class 708, Subclass 530 for Electrical Computers: Arithmetic Processing and Calculating; Error Detection or Correction;
- Class 726, Subclass 22 for Information Security; Monitoring or Scanning of Software or Data Including Attack Prevention;
- Class 726, Subclass 23 for Information Security; Intrusion Detection;
- Class 726, Subclass 24 for Information Security; Virus Detection;
- Class 726, Subclass 25 for Information Security; Vulnerability Assessment;

B. European Patent Office esp@cenet Database

The European Patent Office's esp@cenet classification database for both issued patents and pending applications was searched in the following European Classifications (ECLA):

- H04L12/58F for Electricity; Electric Communication Technique; Transmission of Digital Information; Data Switching Networks; Stored and Forward Switching Systems; Message Switching Systems with Filtering and Selective Blocking Capabilities;

C. The World Intellectual Property Office's

The World Intellectual Property Organization's PatentScope database for published international applications was search in the following International Patent Classifications (IPC):

- G06F for Physics; Computing, Calculating, Counting; Electrical Digital Data Processing;

D. The Japanese Patent Office

The Japanese Patent Office 'Patent Abstracts of Japan' database for both issued patents and pending applications was searched in the following IPC:

- G06F for Physics; Computing, Calculating, Counting; Electrical Digital Data Processing;

E. The Association of Computing Machinery's (ACM) Digital Library

The ACM Digital Library database for articles referring to 'spam' and 'unsolicited commercial e-mail' (and certain variants (*e.g.*, 'UCE'));

F. References Provided by the Applicants

Certain references identified by the Applicants have been previously provided in an *Information Disclosure Statement*. These references have been carefully reviewed and

have been determined to be, by far, less relevant and/or cumulative with respect to the references discussed in the context of MPEP § 708.02(VIII)(E). Notwithstanding, these references are identified below.

V. MPEP § 708.02(VIII)(D)

The references deemed most closely related to the subject matter encompassed by the claims (and a copy thereof in the case of any foreign or non-patent literature) have been submitted to the U.S. Patent Office in an *Information Disclosure Statement* submitted on March 14, 2005 and July 26, 2006.

VI. MPEP § 708.02(VIII)(E)

The Applicants submit, herewith, a detailed discussion of the references, which points out in the particularity requirement by 37 C.F.R. § 1.111(b) and (c). Said discussion identifies how the claimed subject matter is patentable over the references identified herein.

U.S. 6,941,466: ***Method and Apparatus for Providing Automatic E-Mail Filtering Based on Message Semantics, Sender's E-Mail ID, and User's Identity*** **(Mastrianni)**

Mastrianni purportedly provides "a method, computer program product, and apparatus for providing context-aware automatic e-mail filtering and reply generation." 466:1:47-49. More specifically, Mastrianni purports to provide a "semantic engine, which... analyzes the e-mail using filter definitions and then saves, deletes, or forwards the e-mail based on matches or lack of matches between the e-mail and the filter definitions." 466:3:42-46.

The semantic engine is further configured to "observe actions taken by the user and store these actions in a historical data database." 466:3:51-52. Mastrianni purportedly teaches "keeping track of the number of offending e-mail message IDs, domains, and relays, and us[ing] that information to automatically filter offending e-mail messages without any operator intervention." 466:4:48-51. Mastrianni further purports to provide that "using the data in the historical data database, the semantic engine may automatically forward, save, or delete future e-mail messages received that have a user ID, originating IP address, or other characteristic in common with previously received e-mail based on the actions the user took with the previous e-mail." 466:3:53-58.

In Mastrianni, "e-mail containing objectionable content as determined by the presence of objectionable words or phrases or by an objectionable score determined by assigning weights to various words and phrases that exceeds a threshold value [are deleted]." 466:1:54-58. More specifically, "the message is examined by the Semantic Engine for the selected content by topic, such as, for example, gambling, sex, work at home, etc." 466:4:21-22.

With respect to independent claim 1, Mastrianni fails to disclose "*associating* the domain with the IP address." Mastrianni concerns an e-mail filtering mechanism that may refer separately to the user ID and/or the IP

address associated with an incoming message but the semantic engine does not associate these elements to determine a classification of a message. As Mastrianni does not disclose associating the domain with the IP address, there is no classifying the message based on the associated domain and IP address as required by claim 1. Independent claim 35 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. Mastrianni therefore fails to disclose the limitations of claim 35 for at least the same reasons as claim 1. Independent claim 36 concerns a 'system' for 'classifying a message' that is similar in scope to the method of independent claim 1. Mastrianni therefore fails to disclose the limitations of claim 36 for at least the same reasons as claim 1.

With respect to independent claim 12, Mastrianni fails to disclose "a method for determining a boundary IP address." While Mastrianni does disclose "block[ing] the receipt of e-mail messages by IP number," Mastrianni fails to disclose "processing a header to extract a plurality of candidate IP addresses." 466:5:36-37. Further, Mastrianni does not disclose "extract[ing] a plurality of candidate IP addresses." By not extracting a plurality of IP addresses, Mastrianni fails to disclose determining a boundary IP address, as required by claim 12.

U.S. 2006/0015942: *Systems and Methods for Classification of Messaging Entities* (Judge et al.)

Judge et al. concerns purported "methods and systems .:. for operation upon one or more data processors for assigning a reputation to a messaging entity" and for "deciding what action is to be taken with respect to a communication associated with the messaging entity." [0006]. To assign a reputation, "a method can include receiving data that identifies one or more

characteristics related to a messaging entity's communication." [0006]. Judge et al. further discloses that the "reputation score is determined based upon the received identification data" where the "determined reputation score is indicative of reputation of the messaging entity." [0006].

In Judge et al., " a reputation score is computed for a particular sender (e.g., IP address, domain name, phone number, address, name, etc), from a set of input data." [0034]. This "data is gathered ... to calculate non-reputable and reputable probabilities for a sender." [0034]. The probabilities include "determining, for a sender, non-reputable probabilities and reputable probabilities for various selected criteria." [0034].

With respect to independent claim 1, Judge et al. fails to disclose '*associating* the domain with the IP address.' Judge et al. concerns calculating a set of probabilities to determine whether a sender is "reputable." As Judge et al. does not disclose "associating the domain with the IP address," there is no classifying the message based on the associated domain and IP address. Independent claim 35 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. Judge et al. therefore fails to disclose the limitations of claim 35 for at least the same reasons as claim 1. Independent claim 36 concerns a 'system' for 'classifying a message' that is similar in scope to the method of independent claim 1. Judge et al. therefore fails to disclose the limitations of claim 36 for at least the same reasons as claim 1.

With respect to independent claim 12, Judge et al. fails to disclose 'a method for determining a boundary IP address.' Judge et al. also fails to disclose 'extracting a plurality of candidate IP addresses' in such a message thereby preventing 'selecting the boundary IP address.'

U.S. 2004/0267886: *Filtering Email Messages Corresponding to Undesirable Domains* (Malik)

Malik purportedly provides "for filtering email messages originating from undesirable domains, such as, for example, addresses associated with designated geographical areas." [0004] For example, "one embodiment comprises receiving an email message having an originating IP address, extracting the originating IP address from the email message, and comparing the originating IP address to a list of undesirable IP addresses." To determine whether a message should be classified as spam, "the comparison results in a determination of whether or not the extracted email address is included in the list of undesirable IP addresses." [0004].

In some embodiments, the IP address "is extracted from the header of the email message." [0021]. To filter messages having an IP address on the list of undesirable IP addresses, "email attributes are further extracted from the email message. The extracted email attributes are compared to a list of desired email attributes." [0030]. Malik further describes that "for example, the list of desired email attributes may include a particular sender's name, a specific email address of a sender, a specified sender IP address, email content, [or] type of content." [0019].

With respect to independent claim 1, Malik fails to disclose '*associating* the domain with the IP address.' Malik concerns using the IP address to determine how to classify the message. As Malik does not disclose an association of an IP address to a domain, there is no 'classification based on the associated domain and IP address.' Independent claim 35 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. Malik therefore fails to disclose the limitations of claim 35 for at least the same reasons as claim 1. Independent claim 36 concerns a 'system' for

'classifying a message' that is similar in scope to the method of independent claim 1. Malik therefore fails to disclose the limitations of claim 36 for at least the same reasons as claim 1.

With respect to independent claim 12, Malik fails to disclose 'a method for determining a boundary IP address.' Malik also fails to disclose 'locating a gateway IP address' in such a message thereby preventing 'selecting the boundary IP address based on the location of the gateway IP address.'

WO 2005/048033: *System and Method for Managing a Trusted Email Datastore* (Yahoo!)

Yahoo! purports to provide "A Trust Email Datastore (TED) system is employed to maintain a list of message addresses with associated trust ratings." Abstract. Yahoo! discloses that "the trust rating of a message address is derived from an underlying message address relationship network around the message address of interest through various network related activities such as message sending, forwarding, deleting, blocking, marking as is/is not spam, saving to address book, etc." Abstract. The trust rating comprises two components, first, a "relationship trust, may be determined based on proximity of two message addresses in a message address relationship graph." Abstract. "Another component of the trust rating is substantially independent of the positions of two message addresses in the message address relationship graph, and is referred to as a universal trust rating." Abstract.

With respect to independent claim 1, Yahoo! fails to disclose 'a method for classifying a message.' Yahoo! concerns creating and maintaining a trust rating of specific senders. As Yahoo! does not disclose a message for classification, there is no 'association of the domain with the IP address' of a message. As the 'classification of the message based on the associated domain and IP address' is

absent from Yahoo!, there is no determination that the message is classified as is recited in claim 1. Independent claim 35 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. Yahoo! therefore fails to disclose the limitations of claim 35 for at least the same reasons as claim 1. Independent claim 36 concerns a 'system' for 'classifying a message' that is similar in scope to the method of independent claim 1. Yahoo! therefore fails to disclose the limitations of claim 36 for at least the same reasons as claim 1.

With respect to independent claim 12, Yahoo! fails to disclose 'a method for determining a boundary IP address.' Yahoo! also fails to disclose 'locating a gateway IP address' in such a message thereby preventing 'selecting the boundary IP address based on the location of the gateway IP address.

WO 99/33188: *Apparatus and Method for Controlling Delivery of Unsolicited Electronic Mail* (Bright Light Technologies, hereinafter "Bright Light")

Bright Light purports to provide "a method and system for controlling delivery of unsolicited electronic mail messages." Abstract. "One or more spam probe email addresses are created and planted at various sites on the communications network in order to insure their inclusion on large-scale electronic junk mail ("spam") mailing lists." Abstract. "Upon receipt of incoming mail addressed to the spam probe addresses, the spam control center automatically analyzes the received spam e-mail to identify the source of the message, extracts the spam source data from the message, and generates an alert signal containing the spam source data." Abstract.

Bright Light describes "the alert signal may also contain filtering instructions used to enable network servers and user terminals to automatically

detect spam." Summary. "A filtering system implemented at the servers or user terminals automatically receives the alert signal, automatically updates stored filtering data using the source data retrieved from the alert signal, and automatically controls delivery of subsequently received e-mail messages from the identified spam source." Summary.

With respect to independent claim 1, Bright Light fails to disclose 'associating the domain with the IP address.' Bright Light concerns updating and maintaining a filtering system for incoming spam. As Bright Light does not disclose associating the domain with the IP address, there is no 'classification based on the associated domain and IP address.' Independent claim 35 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. Bright Light therefore fails to disclose the limitations of claim 35 for at least the same reasons as claim 1. Independent claim 36 concerns a 'system' for 'classifying a message' that is similar in scope to the method of independent claim 1. Bright Light therefore fails to disclose the limitations of claim 36 for at least the same reasons as claim 1.

With respect to independent claim 12, Bright Light fails to disclose 'a method for determining a boundary IP address.' Bright Light also fails to disclose 'locating a gateway IP address' in such a message thereby preventing 'selecting the boundary IP address based on the location of the gateway IP address.

PAJ 2005-208780: ***Mail Filtering System and URL Black List Dynamic Construction Method to be Used for the Same*** **(NEC Corp.)**

NEC Corp. purportedly provides "a mail filtering device for reducing a management load by increasing the detection rate of an unsolicited bulk email." Problem to be Solved. The mail filtering device includes "a first retrieval means"

that "retrieves the entry of a mail flow rate storage ... based on the transmission original IP address of the text of an electronic mail." Solution. The first retrieval means "increased a corresponding count value by a specific value when the corresponding entry is found." Solution. "A second retrieval means retrieves whether or not the SPAM determination word...is included in the electronic mail." Solution. Further, the disclosure of NEC Corp. "extracts a character string starting with 'http' from the electronic mail and records it in an SPAM determination word storage ... and a URL black list." Solution.

With respect to independent claim 1, NEC Corp. fails to disclose 'associating the domain with the IP address.' NEC Corp. concerns maintaining a count of received emails according to the original IP address and filtering words and/or URLs in incoming spam. As NEC Corp. does not disclose *associating the domain* with the IP address, there is no 'classification based on the associated domain and IP address.' Independent claim 35 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. NEC Corp. therefore fails to disclose the limitations of claim 35 for at least the same reasons as claim 1. Independent claim 36 concerns a 'system' for 'classifying a message' that is similar in scope to the method of independent claim 1. NEC Corp. therefore fails to disclose the limitations of claim 36 for at least the same reasons as claim 1.

With respect to independent claim 12, NEC Corp. fails to disclose 'a method for determining a boundary IP address.' NEC Corp. also fails to disclose 'locating a gateway IP address' in such a message thereby preventing 'selecting the boundary IP address based on the location of the gateway IP address.'

Communications of the ACM: *Spam!*

This ACM article summarizes purported "technical solutions" to "solve the spam problem." Page 78. The article describes filtering solutions based on "filtering messages from known spam senders based on information in message headers." Page 78. Also, "pattern matchers can sometimes identify spam based on information within the body of an email message." The article further provides that "updating filters and supervising a semi-automated filter can be a time consuming endeavor." Page 78. And "once one copy of an unsolicited commercial message is identified, setting filters to detect additional copies is easier." Page 78.

The ACM article discloses that "some ISPs have experimented with filters that reject all messages from nonregistered domains." Page 78. But the article points out that "such filtering can weed out messages with deliberately faked addresses but it may also drop legitimate messages from misconfigured mail servers. Pages 78-79.

With respect to independent claim 1, the ACM article fails to disclose 'a method for classifying a message.' The ACM article concerns the effectiveness of filtering emails. As the ACM article does not disclose a message for classification, there can be no 'association of the domain with the IP address' of a message. As the 'classification of the message based on the associated domain and IP address' is absent from the ACM article, there is no determination that the message is classified as is recited in claim 1. Independent claim 35 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. The ACM article therefore fails to disclose the limitations of claim 35 for at least the same reasons as claim 1. Independent claim 36 concerns a 'system' for 'classifying a message' that is similar in scope to

the method of independent claim 1. The ACM article therefore fails to disclose the limitations of claim 36 for at least the same reasons as claim 1.

With respect to independent claim 12, the ACM article fails to disclose "a method for determining a boundary IP address." The ACM article also fails to disclose "locating a gateway IP address" in such a message thereby preventing 'selecting the boundary IP address based on the location of the gateway IP address.'

Jung et al.: ***An Empirical Study of Spam Traffic and the Use of DNS Blacklists***

Jung et al. purportedly provides an analysis of "address-based filtering, using which one can refuse to accept mail from host that are believed to send spam." Introduction. Further, Jung et al. disclose that "once identified, the IP address of a host engaged in spam delivery is registered in centrally maintained databases." Introduction. To filter spam from incoming messages, "mail recipients can query this database using standard DNS [domain name system] lookups and deny any mails from the hosts that are listed in the database." Introduction. To perform a DNS lookup on a host *a.b.c.d.*, "a DNS lookup is done for the A record of the name *d.c.b.a.*`blacklist-name`." 2.2 Black Lists. In some situations, "MTAs [mail transfer agents] check DNS blacklists to determine whether the party relaying the mail is listed. ... This activity happens *before* the mail is accepted locally." 2.3 DNSBL Clients. In other situations, "filtering is performed *after* mail is accepted." Tests are performed "that parse the 'Received' headers of a given piece of mail and check if the mail has transited any blacklisted hosts."

With respect to independent claim 1, Jung et al. fails to disclose 'associating the domain with the IP address.' Jung et al. concerns updating and

maintaining a database comprising domain names and/or IP addresses. While Jung et al. purports to query IP addresses using DNS lookups, Jung et al. does not disclose *associating the domain with the IP address,* there is no 'classification based on the associated domain and IP address.' Independent claim 35 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. Jung et al. therefore fails to disclose the limitations of claim 35 for at least the same reasons as claim 1. Independent claim 36 concerns a 'system' for 'classifying a message' that is similar in scope to the method of independent claim 1. Jung et al. therefore fails to disclose the limitations of claim 36 for at least the same reasons as claim 1.

With respect to independent claim 12, Jung et al. fails to disclose 'a method for determining a boundary IP address.' Jung et al. also fails to disclose 'locating a gateway IP address' in such a message thereby preventing 'selecting the boundary IP address based on the location of the gateway IP address.'

SMTP+SPF: *Sender Policy Framework* (SPF)

SPF purportedly provides a way to "fight email address forgery and make it easier to identify spams, worms, and viruses." SPF is used "when domain woners designate *sending* mail servers in DNS." This purportedly allows "STMP receivers can distinguish legitimate mail from spam by verifying the envelope sender address against client IP *before* any message data is transmitted." According to SPF, "any connecting client can assert any sender address." SPF is used by an MTA "to verify the envelope sender (STMP MAIL FROM) address during STMP time." Further, "when used to verify headers ... you have to consider Sender and Resent-From as well as just the 'From:' header."

With respect to independent claim 1, SPF fails to disclose '*associating* the domain with the IP address.' SPF concerns *verifying* sender addresses using IP

addresses appearing in a header of a message based on *designated* 'sending mail servers in DNS.' As verifying a sender address in DNS against an IP address is not equivalent to 'associating the domain with the IP address,' SPF does not disclose associating the domain with the IP address, and there is no 'classification based on the associated domain and IP address.' Independent claim 35 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. SPF therefore fails to disclose the limitations of claim 35 for at least the same reasons as claim 1. Independent claim 36 concerns a 'system' for 'classifying a message' that is similar in scope to the method of independent claim 1. SPF therefore fails to disclose the limitations of claim 36 for at least the same reasons as claim 1.

With respect to independent claim 12, SPF fails to disclose 'a method for determining a boundary IP address.' SPF also fails to disclose 'locating a gateway IP address' in such a message thereby preventing 'selecting the boundary IP address based on the location of the gateway IP address.'

Other References

The following references were carefully reviewed and determined to be, by far, less relevant and/or cumulative with respect to the references discussed above:

Patent/Publication No.	Publication Date	Patentee/Inventor
U.S. 7039954	05-02-2006	Lingafelt et al.
U.S. 7024458	04-04-2006	Chan et al.
U.S. 2004/0236838	11-25-2004	Tout
U.S. 2006/0021055	1-26-2006	Judge et al.
GB 2366706	03-13-2002	Content Technologies
WO 01/53965	07-26-2001	Odyssey Development
WO 01/16695	03-08-2001	Katsikas
WO 02/19069	03-07-2002	Content Technologies
WO 2005/041504	05-06-2005	WEB.DE
PAJ 2000-163341	06-16-2000	NEC Corp
PAJ 2003-087327	03-20-2003	SHARP Corp
PAJ 2003-125004	04-25-2003	NEC Corp
PAJ 2004-240945	08-26-2004	DEEPSOFT Co.
PAJ 2004-362559	12-24-2004	MICROSOFT Corp
PAJ 2005-128922	05-19-2005	NEC Corp
PAJ 2005-135024	05-26-2005	Ando
U.S. 6112227	08-29-2000	Heiner
U.S. 6199102	03-06-2001	Cobb
U.S. 2005-0055410	03-10-2005	Landsman et al.
U.S. 2005-0125667	06-09-2005	Sullivan et al.
U.S. 2004-0024639	02-05-2004	Goldman
U.S. 2003-0233418	12-18-2003	Goldman

Patent/Publication No.	Publication Date	Patentee/Inventor
U.S. 2004-0158554	08-12-2004	Trottman
U.S. 6941348	09-06-2005	Petry et al.
U.S. 6650890	11-18-2003	Irlam et al.

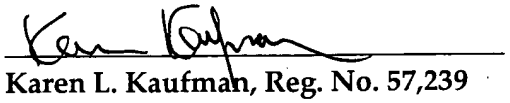
Non-Patent Literature Title	Author	Date
"Spam Wars"	Weinstein	August 2003
"Characterizing a Spam Traffic"	Gomes et al.	October 25-27, 2004
"Razor-agents 2.22"	n/a	n/a
"Spam Filter, A Collaborative Method of Eliminating Spam"	Kolathur et al.	Dec. 8, 2000
"Welcome to Spam Assassin"	n/a	n/a
"The Application of 'Genetic Classification' as a Means to Predict and Extinguish E-mail Spam in the Corporate Enterprise"	Cloudmark Inc.	November 2003
"Brightmail Reputation Service"	Symantec	n/a
"Microsoft Offers Anti-Spam Capabilities to Distinguish Legitimate E-Mail"	Ironport Systems, Inc.	May 5, 2004
"Objections Addressed"	Levine	n/a
"Microsoft Is Committed to Help the Spam Epidemic"	Microsoft	November 16, 2003
"Sender Policy Framework"	AOL Postmaster.info	n/a
"SPF Information"	AOL Postmaster.info	n/a
"Sender Policy Framework"	n/a	n/a
"Pricing via Processing or Combating Junk Mail"	Dwork et al.	1992
"Telling Humans and Computers Apart (Automatically) or how Lazy Cryptographers Do AI"	Von Ahn et al.	February 2004
"How to Make Sure a Human Is Sending you Mail"	Skoll	November 17, 1996
"My Spamblock"	Byrne	January 19,1997
"To Mung or Not to Mung"	Guilmette	July 24, 1997
"Viking-12 Junk Email Blocker"	Templeton	July 15, 2003

Non-Patent Literature Title	Author	Date
"Majordomo FAQ"	n/a	October 20, 2001
"Spam Foe Needs Filter of Himself"	Langberg	April 5, 2003
"In-Boxes That Fight Back"	McCullagh	May 19, 2003
"Cloaking Device Made for Spammers"	McWilliams	October 9, 2003
"The Homograph Attack"	Gabrilovich et al.	n/a
"Protecting Users Against Phishing Attacks with AntiPhish"	Kirda et al.	2005
Characteristics and Responsibilities Involved in a Phishing Attack"	Merwe et al.	2004
FBI Says Web Spoofing Scams are a Growing Problem	FBI	July 21, 2003

VII. Conclusion

The Applicants believe that this Petition to Make Special has met all requirements set forth by 37 C.F.R. § 1.102(d) and MPEP § 708.02(VIII) and respectfully request the petition be granted.

Respectfully submitted,
Jonathan Oliver et al.

July 26, 2006 By: 

Karen L. Kaufman, Reg. No. 57,239
Carr & Ferrell *LLP*
2200 Geng Road
Palo Alto, California 94303
Phone (650) 812-3400
Fax (650) 812-3444